BUNDESREPUBLIK DEUTSCHLAND

CERTIFIED COPY OF
PRIORITY DOCUMENT

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 100 15 389.5

Anmeldetag: 28. März 2000

Anmelder/Inhaber: Philips Corporate Intellectual Property GmbH, Hamburg/DE

Bezeichnung: Drahtloses Netzwerk mit einer Schlüsselwechsel-Synchronisations-Prozedur

IPC: H 04 Q, H 04 L, H 04 B

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 4. September 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hoiß

A 9161
03/00
EDV-L

ZUSAMMENFASSUNG

Drahtloses Netzwerk mit einer Schlüsselwechsel-Synchronisations-Prozedur

Die Erfindung bezieht sich auf ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten über Nutz- und Steuerkanäle und die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten vorgesehen sind. Die Funknetzwerk-Steuerung und wenigstens ein Terminal speichern Dateneinheits-Nummern und kennzeichnen den verwendeten Schlüssels in den Dateneinheiten während einer Synchronisations-Prozedur, die mit der Sendung der ersten mit neuen Schlüssel verschlüsselten Dateneinheit entweder von der Funknetzwerk-Steuerung oder dem Terminal beginnt und mit der wiederholten Sendung der letzten mit alten Schlüssel verschlüsselten Dateneinheit entweder von der Funknetzwerk-Steuerung oder dem Terminal endet.

Fig. 5

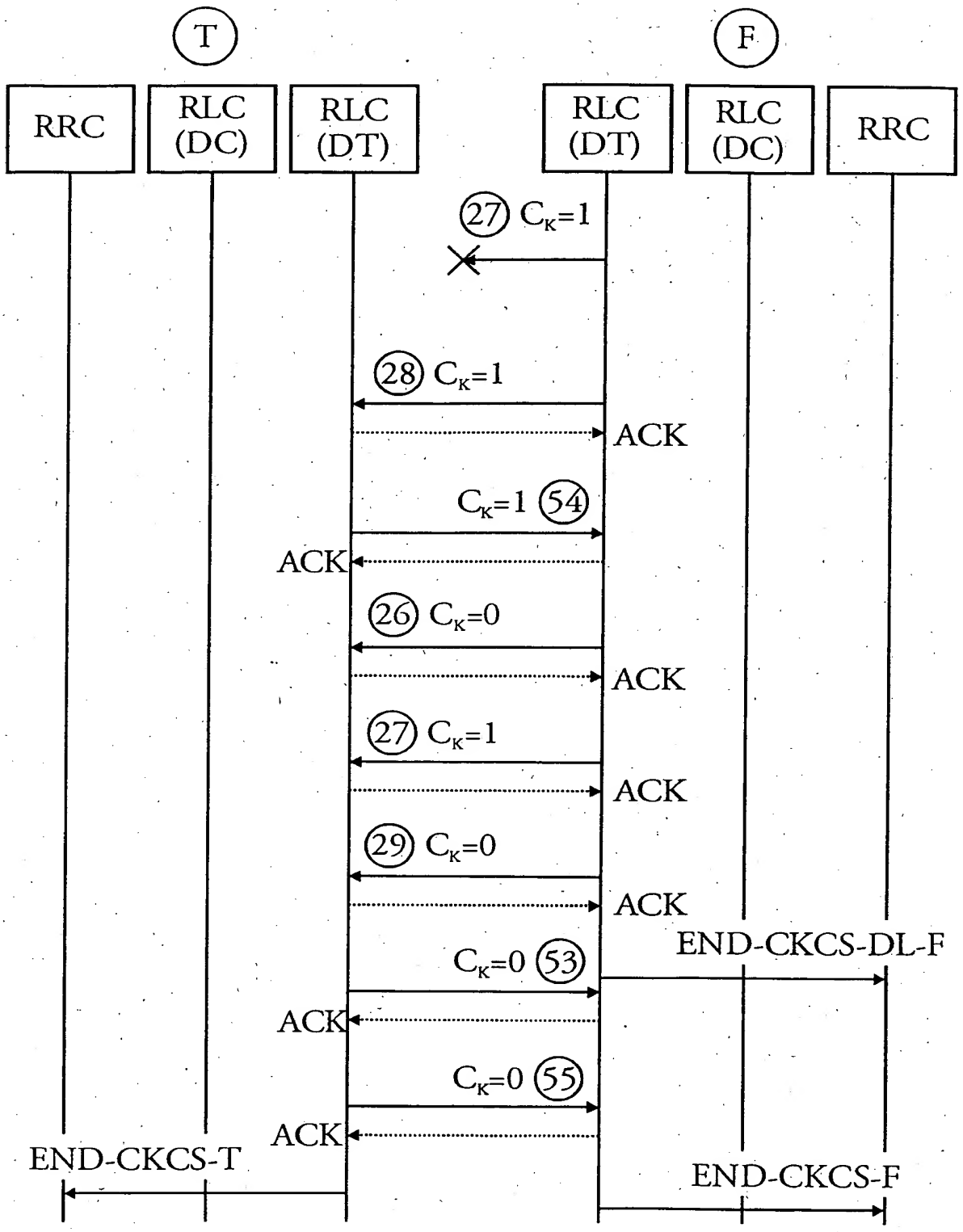
T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
27 C_K=1
28 C_K=1
ACK
C_K=1 54
ACK
26 C_K=0
ACK
27 C_K=1
ACK
29 C_K=0
ACK
END-CKCS-DL-F
C_K=0 53
ACK
C_K=0 55
ACK
END-CKCS-T
END-CKCS-F

FIG. 5

BESCHREIBUNG

Drahtloses Netzwerk mit einer Schlüsselwechsel-Synchronisations-Prozedur

Die Erfindung bezieht sich auf ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten über Nutz- und Steuerkanäle und die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten vorgesehen sind.

Aus dem Buch „The GSM System for Mobile Communications" von Michel Mouly und Marie-Bernadette Pautet, Verlag Cell & Sys, 1992, Seiten 391 bis 395, ist bekannt, dass Daten zwischen einer Basisstation und einem Terminal verschlüsselt übertragen werden. Der für die Übertragung benötigte Schlüssel wird in bestimmten Zeitabständen verändert. Hierfür ist eine Prozedur in drei Schritten vorgesehen.

Der Erfindung liegt die Aufgabe zugrunde, ein drahtloses Netzwerk zu schaffen, das eine andere Prozedur zur Änderung eines Schlüssels angibt.

Die Aufgabe wird durch ein drahtloses Netzwerk der eingangs genannten Art dadurch gelöst,
dass die Funknetzwerk-Steuerung und wenigstens ein Terminal zur Speicherung von Dateneinheits-Nummern und zur Kennzeichnung des verwendeten Schlüssels in den Dateneinheiten während einer Synchronisations-Prozedur vorgesehen sind, die mit der Sendung der ersten mit neuen Schlüssel verschlüsselten Dateneinheit entweder von der Funknetzwerk-Steuerung oder dem Terminal beginnt und mit der wiederholten Sendung der letzten mit alten Schlüssel verschlüsselten Dateneinheit entweder von der Funknetzwerk-Steuerung oder dem Terminal endet.

Unter dem erfindungsgemäßen drahtlosen Netzwerk ist ein Netzwerk mit mehreren Funkzellen zu verstehen, in denen jeweils eine Basisstation und mehrere Terminals Steuer- und Nutzdaten drahtlos übertragen. Eine drahtlose Übertragung dient zur Übertragung von Informationen z.B. über Funk-, Ultraschall- oder Infrarotwege.

6

Erfindungsgemäß wird während einer Synchronisations-Prozedur sichergestellt, dass eine zuvor mit dem alten Schlüssel verschlüsselte und gesendete Dateneinheit, deren Empfang entweder von der Funknetzwerk-Steuerung oder einem Terminal nicht bestätigt worden ist, nach der erstmaligen Sendung von mit dem neuen Schlüssel verschlüsselten anderen Dateneinheiten erneut mit dem alten Schlüssel verschlüsselt gesendet wird. Diese erneute Übertragung einer Dateneinheit mit dem alten Schlüssel wird durch Speicherung von Dateneinheits-Nummern und durch Kennzeichnung der Dateneinheiten erreicht. Die Kennzeichnung, die beispielsweise ein Bit in einem Steuerungsteil der Dateneinheit sein kann, gibt an, ob eine Dateneinheit mit dem alten oder neuen Schlüssel verschlüsselt worden ist. Die Speicherung der Dateneinheits-Nummern ist nötig, um festzustellen, wann diese Synchronisations-Prozedur beendet ist.

Ausführungsbeispiele der Erfindung werden nachstehend anhand der Fig. näher erläutert. Es zeigen:

Fig. 1	ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren Terminals,
Fig. 2	ein Schichtenmodell zur Erläuterung verschiedener Funktionen eines Terminals oder einer Funknetzwerk-Steuerung,
Fig. 3	ein Blockschaltbild zur Erläuterung des Verschlüsselungsmechanismus in einem Terminal oder einer Funknetzwerk-Steuerung und
Fig. 4 und 5	Abläufe verschiedener Befehle bei einer Synchronisations-Prozedur des für die Verschlüsselung benötigten Schlüssels.

In Fig. 1 ist ein drahtloses Netzwerk, z.B. Funknetzwerk, mit einer Funknetzwerk-Steuerung (Radio Network Controller = RNC) 1 und mehreren Terminals 2 bis 9 dargestellt. Die Funknetzwerk-Steuerung 1 ist für Steuerung aller am Funkverkehr beteiligten Komponenten verantwortlich, wie z.B. der Terminals 2 bis 9. Ein Steuer- und Nutzdatenaustausch findet zumindest zwischen der Funknetzwerk-Steuerung 1 und den Terminals 2 bis 9 statt. Die Funknetzwerk-Steuerung 1 baut jeweils eine Verbindung zur Übertragung von Nutzdaten auf.

In der Regel sind die Terminals 2 bis 9 Mobilstationen und die Funknetzwerk-Steuerung 1 ist fest installiert. Eine Funknetzwerk-Steuerung 1 kann gegebenenfalls aber auch beweglich bzw. mobil sein.

In dem drahtlosen Netzwerk werden beispielsweise Funksignale nach dem FDMA-, TDMA- oder CDMA-Verfahren (FDMA = frequency division multiplex access, TDMA = time division multiplex access, CDMA = code division multiplex access) oder nach einer Kombination der Verfahren übertragen.

Beim CDMA-Verfahren, das ein spezielles Code-Spreiz-Verfahren (code spreading) ist, wird eine von einem Anwender stammende Binärinformation (Datensignal) mit jeweils einer unterschiedlichen Codesequenz moduliert. Eine solche Codesequenz besteht aus einem pseudo-zufälligen Rechtecksignal (pseudo noise code), dessen Rate, auch Chiprate genannt, in der Regel wesentlich höher als die der Binärinformation ist. Die Dauer eines Rechteckimpulses des pseudo-zufälligen Rechtecksignals wird als Chipintervall T_C bezeichnet. $1/T_C$ ist die Chiprate. Die Multiplikation bzw. Modulation des Datensignals mit dem pseudo-zufälligen Rechtecksignal hat eine Spreizung des Spektrums um den Spreizungsfaktor $N_C = T/T_C$ zur Folge, wobei T die Dauer eines Rechteckimpulses des Datensignals ist.

Nutzdaten und Steuerdaten zwischen wenigstens einem Terminal (2 bis 9) und der Funknetzwerk-Steuerung 1 werden über von der Funknetzwerk-Steuerung 1 vorgegebene Kanäle übertragen. Ein Kanal ist durch einen Frequenzbereich, einen Zeitbereich und z.B. beim CDMA-Verfahren durch einen Spreizungscode bestimmt. Die Funkverbindung von der Funknetzwerk-Steuerung 1 zu den Terminals 2 bis 9 wird als Downlink und von den Terminals zur Basisstation als Uplink bezeichnet. Somit werden über Downlink-Kanäle Daten von der Basisstation zu den Terminals und über Uplink-Kanäle Daten von Terminals zur Basisstation gesendet.

Beispielsweise kann ein Downlink-Steuerkanal vorgesehen sein, der benutzt wird, um von der Funknetzwerk-Steuerung 1 Steuerdaten vor einem Verbindungsaufbau an alle Terminals 2 bis 9 zu verteilen. Ein solcher Kanal wird als Downlink-Verteil-Steuerkanal

(broadcast control channel) bezeichnet. Zur Übertragung von Steuerdaten vor einem Verbindungsaufbau von einem Terminal 2 bis 9 zur Funknetzwerk-Steuerung 1 kann beispielsweise ein von der Funknetzwerk-Steuerung 1 zugewiesener Uplink-Steuerkanal verwendet werden, auf den aber auch andere Terminals 2 bis 9 zugreifen können. Ein Uplink-Kanal, der von mehreren oder allen Terminals 2 bis 9 benutzt werden kann, wird als gemeinsamer Uplink-Kanal (common uplink channel) bezeichnet. Nach einem Verbindungsaufbau z.B. zwischen einem Terminal 2 bis 9 und der Funknetzwerk-Steuerung 1 werden Nutzdaten über einen Downlink- und ein Uplink-Nutzkanal übertragen. Kanäle, die nur zwischen einem Sender und einem Empfänger aufgebaut werden, werden als dedizierte Kanäle bezeichnet. In der Regel ist ein Nutzkanal ein dedizierter Kanal, der von einem dedizierten Steuerkanal zur Übertragung von verbindungsspezifischen Steuerdaten begleitet werden kann.

Zur Einbindung eines Terminals 2 bis 9 zu einer Funknetzwerk-Steuerung 1 ist ein kollisionsbehafteter Kanal zuständig, der im folgenden als signalisierter RACH-Kanal (RACH = Random Access Channel) bezeichnet wird. Über einen solchen signalisierten RACH-Kanal können auch Dateneinheiten übertragen werden.

Damit Nutzdaten zwischen der Funknetzwerk-Steuerung 1 und einem Terminal ausgetauscht werden können, ist es erforderlich, dass ein Terminal 2 bis 9 mit der Funknetzwerk-Steuerung 1 synchronisiert wird. Beispielsweise ist aus dem GSM-System (GSM = Global System for Mobile communication) bekannt, in welchem eine Kombination aus FDMA- und TDMA-Verfahren benutzt wird, dass nach der Bestimmung eines geeigneten Frequenzbereichs anhand vorgegebener Parameter die zeitliche Position eines Rahmens bestimmt wird (Rahmensynchronisation), mit dessen Hilfe die zeitliche Abfolge zur Übertragung von Daten erfolgt. Ein solcher Rahmen ist immer für die Datensynchronisation von Terminals und Basisstation bei TDMA-, FDMA- und CDMA-Verfahren notwendig. Ein solcher Rahmen kann verschiedene Unter- oder Subrahmen enthalten oder mit mehreren anderen aufeinanderfolgenden Rahmen einen Superrahmen bilden. Aus Vereinfachungsgründen wird im folgenden von einem Rahmen ausgegangen, der als Referenzrahmen bezeichnet wird.

Die Steuer- und Nutzdatenaustausch über die Funkschnittstelle zwischen der Funknetzwerk-Steuerung 1 und den Terminals 2 bis 9 kann mit dem in Fig. 2 dargestellten, beispielhaften Schichtenmodell oder Protokollarchitektur (vgl. z.B. 3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) RAN; Working Group 2 (WG2); Radio Interface Protocol Architecture; TS 25.301 V3.2.0 (1999-10)) erläutert werden. Das Schichtenmodell besteht aus drei Protokollschichten: der physikalischen Schicht PHY, der Datenverbindungsschicht mit den Unterschichten MAC und RLC (in Fig. 2 sind mehrere Ausprägungen der Unterschicht RLC dargestellt) und der Schicht RRC. Die Unterschicht MAC ist für die Medienzugriffssteuerung (Medium Access Control), die Unterschicht RLC für die Funkverbindungssteuerung (Radio Link Control) und die Schicht RRC für die Funkverwaltungssteuerung (Radio Resource Control) zuständig. Die Schicht RRC ist für die Signalisierung zwischen den Terminals 2 bis 9 und der Funknetzwerk-Steuerung 1 verantwortlich. Die Unterschicht RLC dient zur Steuerung einer Funkverbindung zwischen einem Terminal 2 bis 9 und der Funknetzwerk-Steuerung 1. Die Schicht RRC steuert die Schichten MAC und PHY über Steuerungsverbindungen 10 und 11. Hiermit kann die Schicht RRC die Konfiguration der Schichten MAC und PHY steuern. Die physikalische Schicht PHY bietet der MAC-Schicht Transportverbindungen 12 an. Die MAC-Schicht stellt der RLC-Schicht logische Verbindungen 13 zur Verfügung. Die RLC-Schicht ist über Zugangspunkte 14 von Applikationen erreichbar.

Bei einem solchen drahtlosen Netzwerk werden die Daten aus Sicherheits- und Vertraulichkeitsgründen verschlüsselt über die Funkschnittstelle übertragen, um eine Abhören der Daten zu verhindern. Die Verschlüsselung wird in der Datenverbindungsschicht (z. B. in der RLC- oder MAC-Schicht) durchgeführt. Wie Fig. 3 zeigt, werden die Daten D über eine Exklusiv-Oder-Funktion (XOR) mit einer Verschlüsselungsmaske M verknüpft, so dass sich ein verschlüsselter Datenstrom C_D ergibt. Die Verschlüsselungsmaske M wird in einer Verschlüsselungs-Funktion 16 gebildet, die nach einem Verschlüsselungs-Algorithmus arbeitet und als Eingangswerte den Schlüssel CK und andere hier nicht näher dargestellte Parameter P erhält.

Der Schlüssel muss sowohl der Funknetzwerk-Steuerung 1 als auch den Terminals 2 bis 9 bekannt sein. Dieser Schlüssel wird zu bestimmten Zeitpunkten (z.B. alle 2 Stunden)

geändert. Hierbei werden lokale Meldungen zwischen den Schichten RLC und RRC übertragen. Die Schicht RLC verfügt über zwei Instanzen RLC(DC) und RLC(DT). Die Instanz RLC(DT) ist für die Steuerung von dedizierten Nutzkanälen (dedicated traffic channel = DTCH) und die Instanz RLC(DC) für die Steuerung von dedizierten Steuerungskanälen (dedicated control channel = DCCH) zuständig. Das Terminal erhält die Information über den neuen Schlüssel in einer separaten Authentifizierungs-Prozedur zwischen Terminal und Funknetzwerk-Steuerung, wie sie beispielsweise in GSM beschrieben ist (vgl. „GSM Global System for Mobile Communication" von J. Eberspächer und H.-J. Vogel, Teubner Stuttgart 1997, Seiten 146 bis154) . Hierbei wird vermieden, dass der Schlüssel selbst über die Funkschnittstelle übertragen wird.

Mit einer speziellen Prozedur CKCS (cipher key change synchronisation), die als Synchronisations-Prozedur bezeichnet wird, wird dann ein synchronisiertes Umschalten vom alten auf den neuen Schlüssel zwischen Terminal und Funknetzwerk-Steuerung durchgeführt. Die Synchronisations-Prozedur CKCS beginnt mit einer Prolog-Phase, der sich eine Synchronisations-Phase anschließt. Die Fig. 4 und 5 zeigen verschiedene Meldungen, die zwischen den Schichten RRC und RLC eines Terminals (linke Seite der Fig. 4 und 5, mit „T" angegeben) und der Funknetzwerk-Steuerung (rechte Seite der Fig. 4 und 5, mit „F" angegeben) gesendet werden.

Zuerst wird von der Funknetzwerk-Steuerung (vgl. Fig. 4) das Terminal über den beabsichtigten Wechsel zum neuen Schlüssel informiert. Auf der Seite F beauftragt dazu die Schicht RRC die Instanz RLC(DC) mit der lokalen Meldung AMD-REQ-CCC eine Nachricht AMD-PDU-CCC an die Instanz RLC(DC) der Seite T zu senden. Diese Instanz informiert die Instanz RLC(DC) der Seite F mit der Empfangsbestätigung ACK und die Schicht RRC der Seite T mit der lokalen Meldung AMD-REQ-CCC über die empfangene Nachricht. Auf der Seite F wird die Empfangsbestätigung ACK von RLC(DC) über die lokale Meldung AMD-CON-CCC an RRC weitergereicht.

Auf der Seite T beauftragt dazu die Schicht RRC die Instanz RLC(DC) mit der lokalen Meldung AMD-REQ-CCOK eine Nachricht AMD-PDU-CCOK an die Instanz RLC(DC) der Seite F zu senden. RLC(DC) der Seite F informiert die Instanz RLC(DC)

der Seite T mit der Empfangsbestätigung ACK und die Schicht RRC der Seite F mit der lokalen Meldung AMD-IND-CCOK über die empfangene Nachricht. Auf der Seite T wird die Empfangsbestätigung ACK von RLC(DC) über die lokale Meldung AMD-CON-CCOK an die Schicht RRC weitergereicht.

Der bisher beschriebene Meldungs- und Nachrichtenaustausch wird als Prolog der Prozedur CKCS bezeichnet. Die Nachrichten AMD-PDU-CCC und AMD-PDU-CCOK werden mit dem alten Schlüssel verschlüsselt. Diese Nachrichten weisen einen Steuerungsteil mit Steuerungsinformationen auf, der als RLC-Header bezeichnet wird. Ein spezielles Bit C_K dieses RLC-Headers zeigt an, ob der neue oder alte Schlüssel verwendet wird. Durch Verwendung dieses speziellen Bits C_K ist es möglich, dass eine Dateneinheit, die schon einmal vor der Prozedur CKCS übertragen und dessen Empfang noch nicht bestätigt worden ist, erneut mit dem alten Schlüssel übertragen werden kann. Dateneinheiten werden mit dem neuen Schlüssel verschlüsselt, wenn sie zum ersten Mal nach dem Prolog gesendet werden. Durch diese Maßnahme hört ein Lauscher bei Übertragungswiederholungen immer nur identische Kopien von schon einmal empfangenen verschlüsselten Dateneinheiten und erhält keine neuen Information, wenn er in der Phase einer Übertragungswiederholung den Kanal abhört.

Vor dem Prolog der Prozedur CKCS ist dieses spezielle Bit C_K auf Null gesetzt. Nach dem Prolog zeigt in der folgenden Synchronisations-Phase das auf Eins gesetzte spezielle Bit C_K an, dass die Daten mit dem neuen Schlüssel verschlüsselt wurden, während das auf Null gesetzte Bit C_K in der Synchronisations-Phase bedeutet, dass die Daten mit dem alten Schlüssel verschlüsselt wurden.

Die Synchronisations-Phase beginnt im Terminal und in der Funknetzwerksteuerung zu unterschiedlichen Zeiten: Im Downlink (DL) beginnt die Synchronisations-Phase mit der Übertragung der ersten Dateneinheit DL-new-new, nachdem die Schicht RRC den Instanzen RLC(DC) und RLC(DT) der Schicht RLC über die lokalen Meldungen START-CKCS-DL und START-CKCS-DT den Beginn der Synchronisations-Phase mitgeteilt hat. Eine (auf dem Downlink geschicktes) Dateneinheit heißt DL-new-new, wenn es zum ersten Mal nach dem Prolog übertragen wird. Eine Dateneinheit DL-new-new wird zu

einer Dateneinheit DL-new, sobald eine Übertragungswiederholung erfolgt. Eine Dateneinheit wird als DL-old-old bezeichnet, wenn es schon vor dem Prolog (erstmals oder wiederholt) übertragen wurde. Es wird als DL-old bezeichnet, wenn es nach dem Prolog erneut übertragen wird.

Im Uplink (UL) beginnt die Synchronisations-Phase mit der Übertragung der ersten Dateneinheit UL-new-new. Eine (auf dem Uplink) geschickte Dateneinheit heißt UL-new-new, wenn sie zum ersten Mal nach dem Empfang der ersten Dateneinheit DL-new-new oder DL-new verschickt wird. Diese wird als Dateneinheit UL-new bezeichnet, sobald sie erneut übertragen wird. Eine Dateneinheit heißt UL-old-old, wenn diese vor dem Empfang der ersten Dateneinheit DL-new-new oder DL-new übertragen wird. Sie heißt Dateneinheit UL-old, wenn es sich um die erneute Übertragung einer Dateneinheit DL-old-old nach dem Empfang der ersten Dateneinheit DL-new-new oder DL-new handelt.

Die folgenden Regeln 1 bis 5 steuern die Synchronisations-Phase derart, dass das spezielle Bit C_K auf den Wert Null gesetzt werden kann und die entsprechende Dateneinheit nur noch mit dem neuen Schüssel verschlüsselt übertragen werden, nachdem sowohl im Uplink als auch im Downlink alle Dateneinheiten UL-old und DL-old entweder erfolgreich (mit dem alten Schlüssel verschlüsselt) übertragen wurden oder die Maximalzahl der erlaubten Übertragungswiederholungen für diese Dateneinheiten erreicht wurde. Wenn die Maximalzahl erreicht worden ist, wird nicht weiter versucht, diese zu übertragen.

<u>Regel 1:</u>

Während der Synchronisations-Phase im Downlink sendet die RLC-Schicht (z.B. Instanz RLC(DT)) der Seite F mit dem neuen Schlüssel verschlüsselte Dateneinheiten DL-new-new und DL-new. Das spezielle Bit C_K ist gleich Eins gesetzt. Dateneinheiten DL-old werden dagegen mit dem alten Schlüssel verschlüsselt gesendet, wobei das spezielle Bit C_K gleich Null gesetzt ist. In Fig. 5 hat eine solche Dateneinheit die Dateneinheits-Nummer 26. Während der Synchronisations-Phase im Uplink sendet die RLC-Schicht (z.B. Instanz RLC(DT)) mit dem neuen Schlüssel verschlüsselte Dateneinheiten UL-new-new und UL-new, wobei das spezielle Bit C_K gleich Eins gesetzt ist. Dateneinheiten UL-old werden mit dem alten Schlüssel verschlüsselt gesendet, wobei das spezielle Bit C_K gleich Null gesetzt ist.

Regel 2:

Die RLC-Schicht speichert die laufende Dateneinheits-Nummer SN (sequence number) der ersten fehlerfrei empfangenen Dateneinheit DL-new-new oder DL-new. Diese Dateneinheits-Nummer ist Bestandteil des RLC-Headers und wird auf der Seite T als $SN_{F\text{-}DL}(T)$ bezeichnet.

In Fig. 4 weist $SN_{F\text{-}DL}(T)$ die Dateneinheits-Nummer 28 auf. Die zuvor gesendete Dateneinheit DL-new-new mit der Dateneinheits-Nummer 27 (Fig. 4) wurde nicht fehlerfrei übertragen. Wenn die Dateneinheit mit der Dateneinheits-Nummer 27 erneut übertragen wird, wird diese zu einer Dateneinheit DL-new.

Die RLC-Schicht der Seite F speichert die laufende Dateneinheits-Nummer der ersten quittierten Dateneinheit DL-new-new oder DL-new. Diese Dateneinheits-Nummer wird mit $SN_{F\text{-}DL}(F)$ bezeichnet. In Fig. 4 hat $SN_{F\text{-}DL}(F)$ ebenfalls den Wert 28 und gehört zu einer Dateneinheit DL-new-new.

Regel 3:

Die RLC-Schicht der Seite F speichert die laufende Nummer der ersten fehlerfrei empfangenen Dateneinheit UL-new-new oder UL-new. Diese Nummer wird mit $SN_{F\text{-}UL}(F)$ bezeichnet. In Figur 4 hat sie den Wert 54 und stammt von einer Dateneinheit UL-new-new, während die Dateneinheit mit der Dateneinheits-Nummer 53 eine Dateneinheit UL-old ist.

Im allgemeinen gilt:

$$SN_{F\text{-}DL}(T) \leq SN_{F\text{-}DL}(F) \text{ und}$$
$$SN_{F\text{-}UL}(F) \leq SN_{F\text{-}UL}(T).$$

Diese Dateneinheits-Nummern $SN_{F\text{-}DL}(T)$, $SN_{F\text{-}DL}(F)$, $SN_{F\text{-}UL}(F)$ und $SN_{F\text{-}UL}(T)$ werden während der Prolog-Phase mit ungültigen Werten belegt. Jede aus einem RLC-Header einer Dateneinheit entnommene Dateneinheits-Nummer ist ein gültiger Wert.

Regel 4:

Erst wenn $SN_{F\text{-}UL}(F)$ einen gültigen Wert erhalten hat, kann die Synchronisations-Phase im Downlink beendet werden. Sie endet, sobald die RLC-Schicht der Seite F Quittungen für alle Dateneinheiten DL-old und DL-new erhalten hat oder die Maximalzahl von Übertragungswiederholungen aller Dateneinheiten DL-old oder DL-new erreicht wurde. Da die RLC-Schicht der Seite F alle Dateneinheiten kennt, die irgendwann einmal auf dem Downlink verschickt wurden, kann sie diese Entscheidung treffen. Das Ende der Synchronisations-Phase im Downlink wird der RRC-Schicht der Seite F durch die Meldung END-CKCS-DL-F mitgeteilt.

Das Ende der Synchronisations-Phase im Downlink wird der Seite T dadurch angezeigt, dass Dateneinheit DL-new-new mit dem auf Null gesetzten speziellen Bit C_K gesendet werden, aber mit dem neuen Schlüssel verschlüsselt sind. In Fig. 5 hat die erste so gesendete Dateneinheit die Dateneinheits-Nummer 29. Die RLC-Schicht der Seite T erkennt das Ende der Synchronisations-Phase im Downlink daran, dass die Dateneinheits-Nummer der Dateneinheit, die mit dem auf 0 gesetzten speziellen Bit C_K empfangenen wurde, größer oder gleich dem gespeicherten Wert $SN_{F\text{-}DL}(T)$ ist.

Nach dem Ende der Synchronisations-Phase im Downlink sendet die RLC-Schicht der Seite F alle Dateneinheiten verschlüsselt mit dem neuen Schlüssel und mit dem auf Null gesetzten speziellen Bit C_K. Die RLC-Schicht der Seite T empfängt dann nur noch mit dem neuen Schlüssel verschlüsselte Dateneinheiten.

Regel 5:

Die RLC-Schicht der Seite T erkennt das Ende der Synchronisations-Phase im Uplink daran, dass alle Dateneinheiten UL-old oder UL-new entweder quittiert worden sind oder die Maximalzahl von Übertragungswiederholungen für diese Dateneinheiten erreicht wurde. Das Ende der Synchronisations-Phase im Uplink wird der RRC-Schicht der Seite T durch die Meldung END-CKCS-T mitgeteilt.

Das Ende der Synchronisations-Phase im Uplink wird der Seite F dadurch angezeigt, dass eine Dateneinheit UL-new-new mit dem auf Null gesetzten speziellen Bit C_K gesendet

wird, aber mit dem neuen Schlüssel verschlüsselt ist. In Fig. 5 hat die erste so gesendete Dateneinheit die Dateneinheits-Nummer 55. Die RLC-Schicht der Seite F erkennt das Ende der Synchronisations-Phase im Uplink daran, dass die Dateneinheits-Nummer der Dateneinheit, welche mit dem auf Null gesetzten speziellen Bit C_K empfangen wurde, größer oder gleich dem gespeicherten Wert $SN_{F\text{-}UL}(F)$ ist. Das Ende der Synchronisations-Phase im Uplink wird der RRC-Schicht der Seite F durch die Meldung END-CKCS-F mitgeteilt, damit überhaupt wieder eine neue Prozedur CKCS gestartet werden kann.

Nach dem Ende der Synchronisations-Phase im Uplink sendet die RLC-Schicht der Seite T alle Dateneinheiten verschlüsselt mit dem neuen Schlüssel und mit dem auf Null gesetzten speziellen Bit C_K. Die RLC-Schicht der Seite F empfängt dann nur noch mit dem neuen Schlüssel verschlüsselte Dateneinheiten.

Durch Verwendung des speziellen Bits C_K wird erreicht , dass die Prozedur CKCS keine Unterbrechung der Übertragung verursacht. Ohne die Verwendung der gespeicherten Werte $SN_{F\text{-}DL}(T)$, $SN_{F\text{-}DL}(F)$, $SN_{F\text{-}UL}(F)$ und $SN_{F\text{-}UL}(T)$ ist die Beendigung der Prozedur CKCS nicht fehlerfrei möglich.

PATENTANSPRÜCHE

1. Drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten über Nutz- und Steuerkanäle und die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten vorgesehen sind,
dadurch gekennzeichnet,
dass die Funknetzwerk-Steuerung und wenigstens ein Terminal zur Speicherung von Dateneinheits-Nummern und zur Kennzeichnung des verwendeten Schlüssels in den Dateneinheiten während einer Synchronisations-Prozedur vorgesehen sind, die mit der Sendung der ersten mit neuen Schlüssel verschlüsselten Dateneinheit entweder von der Funknetzwerk-Steuerung oder dem Terminal beginnt und mit der wiederholten Sendung der letzten mit alten Schlüssel verschlüsselten Dateneinheit entweder von der Funknetzwerk-Steuerung oder dem Terminal endet.

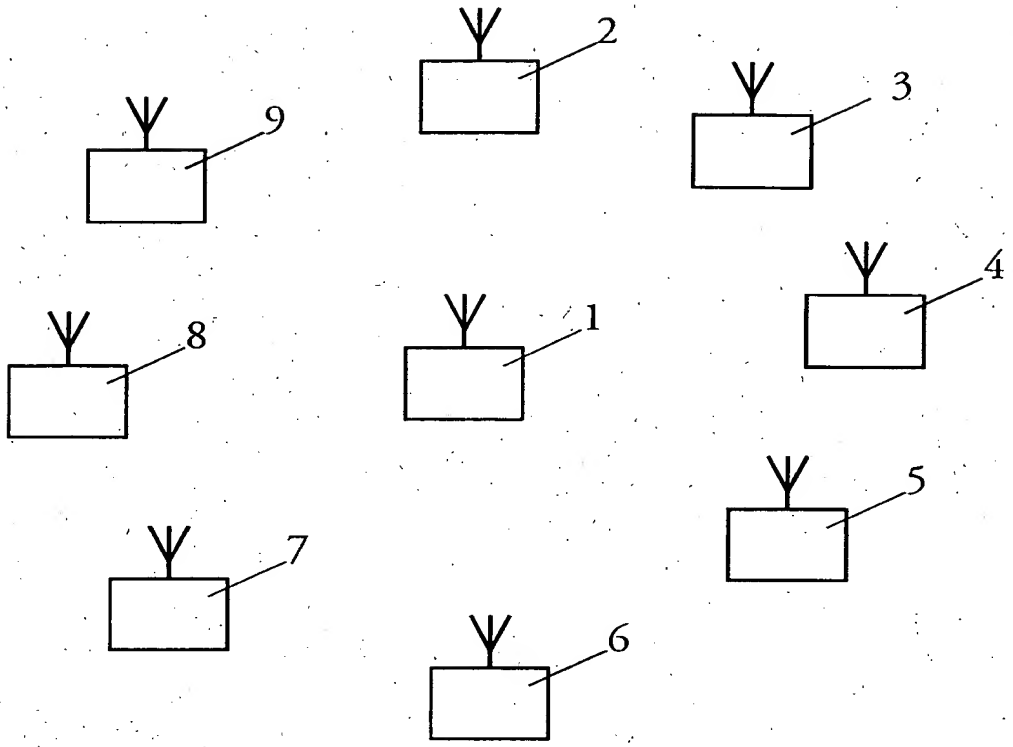

FIG. 1

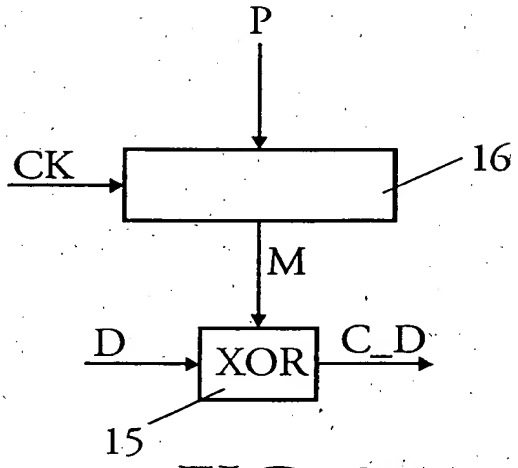

FIG. 3

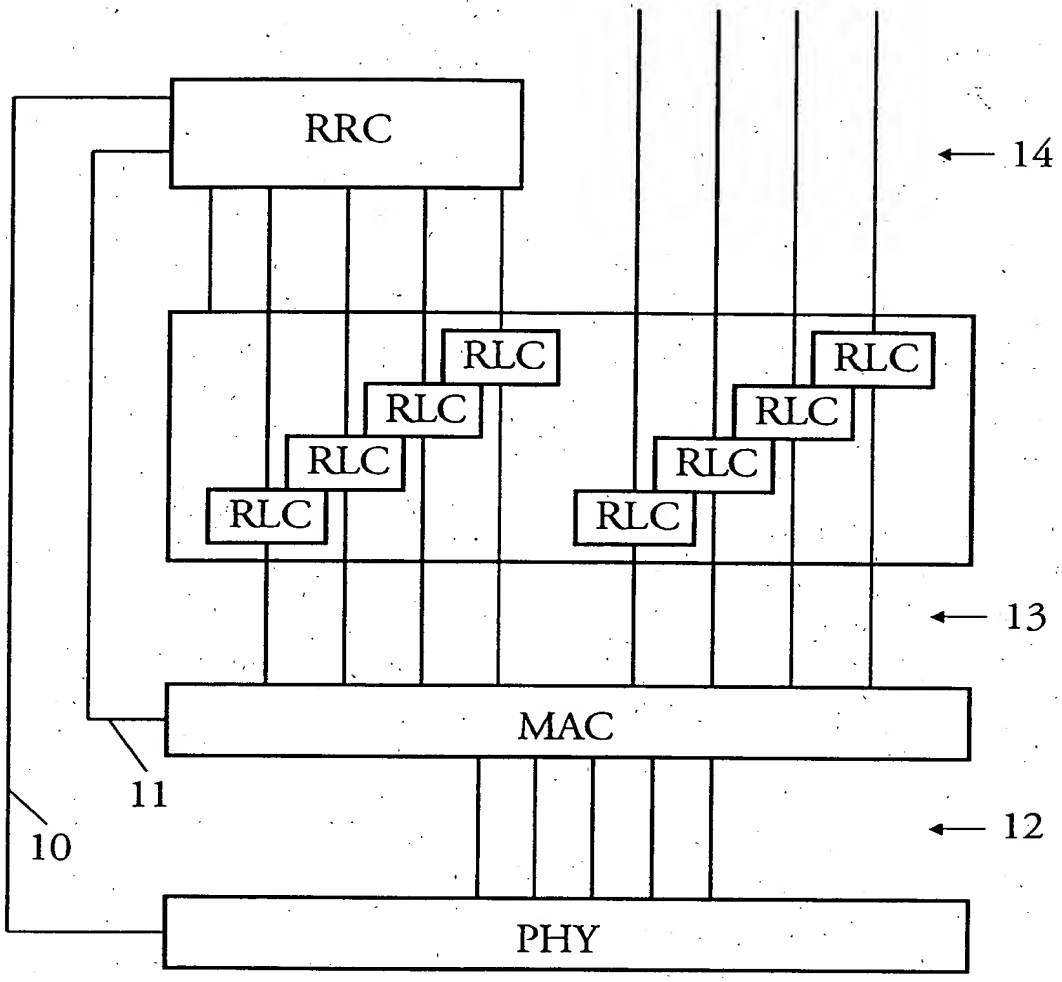

FIG. 2

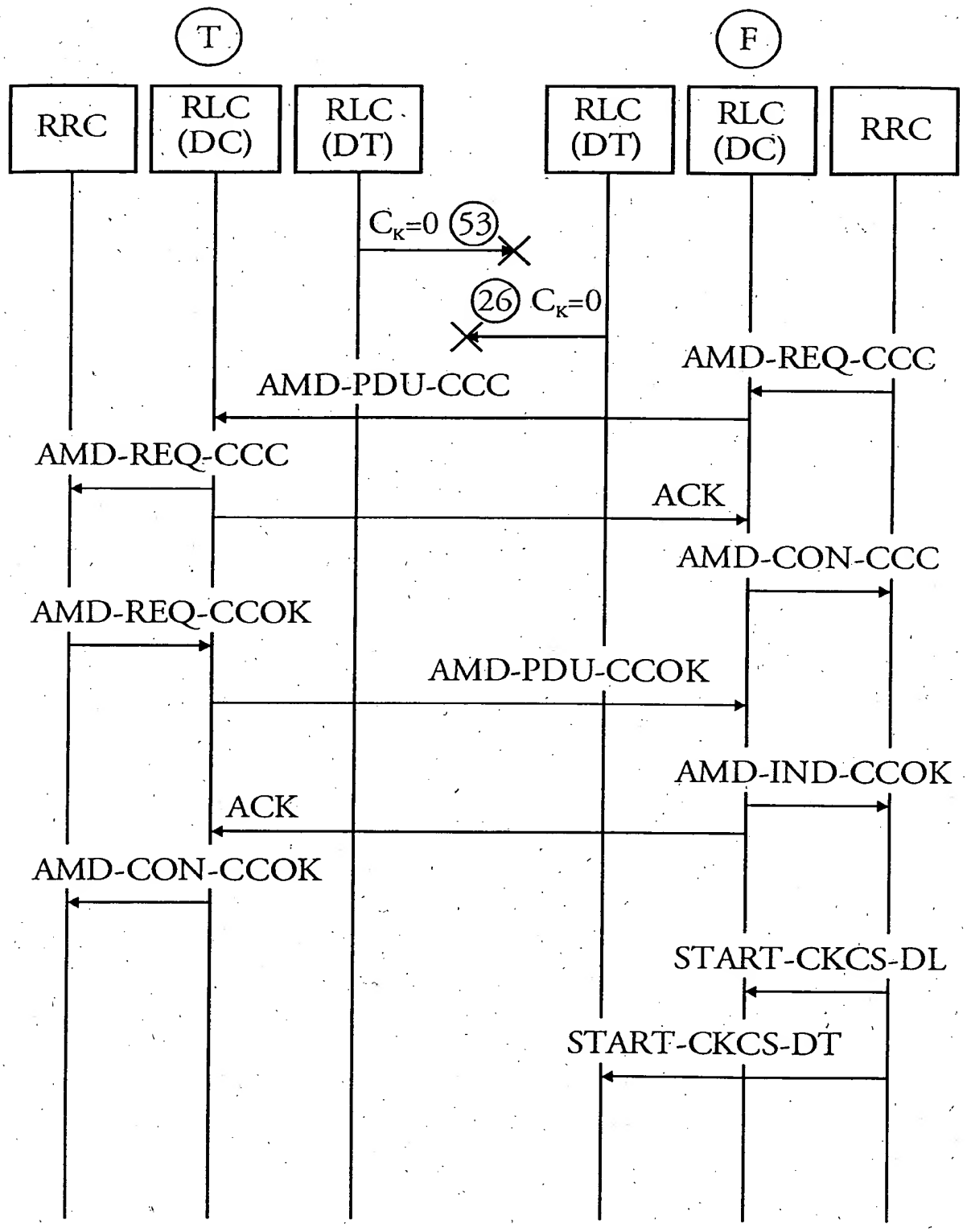
T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
C_K=0 53
26 C_K=0
AMD-REQ-CCC
AMD-PDU-CCC
AMD-REQ-CCC
ACK
AMD-CON-CCC
AMD-REQ-CCOK
AMD-PDU-CCOK
AMD-IND-CCOK
ACK
AMD-CON-CCOK
START-CKCS-DL
START-CKCS-DT

FIG. 4

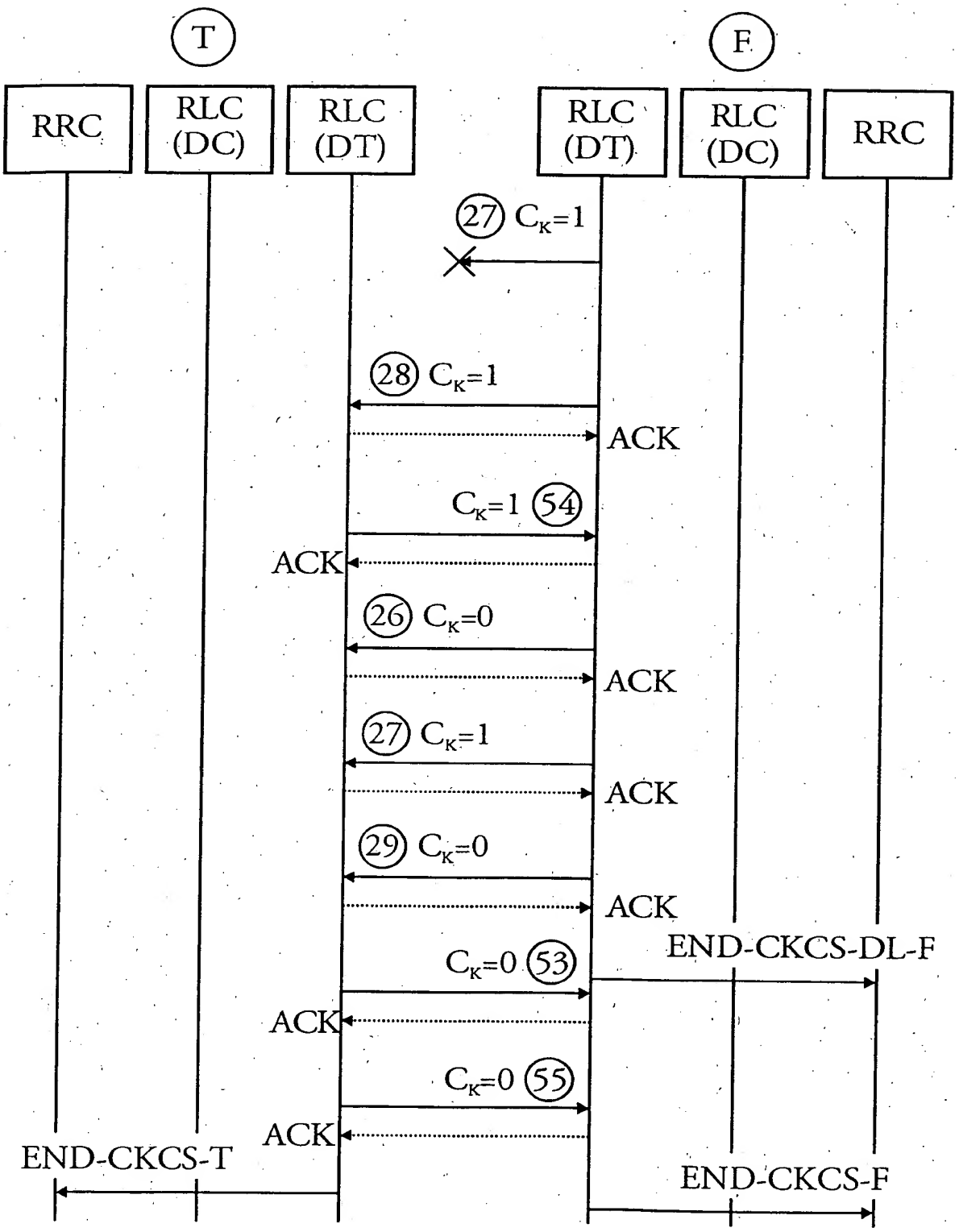
T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
27 C_K=1
28 C_K=1
ACK
C_K=1 54
ACK
26 C_K=0
ACK
27 C_K=1
ACK
29 C_K=0
ACK
END-CKCS-DL-F
C_K=0 53
ACK
C_K=0 55
ACK
END-CKCS-T
END-CKCS-F

FIG. 5